MC 2.40-54

MINISTÉRIO DA DEFESA

EXÉRCITO BRASILEIRO

COMANDO DE OPERAÇÕES TERRESTRES

Manual de Campanha

INTELIGÊNCIA DE FONTES ABERTAS

1ª Edição
2025

MC 2.40-54

MINISTÉRIO DA DEFESA

EXÉRCITO BRASILEIRO

COMANDO DE OPERAÇÕES TERRESTRES

Manual de Campanha

INTELIGÊNCIA DE FONTES ABERTAS

1ª Edição
2025

PORTARIA – COTER/C Ex Nº Nº 531, DE 24 DE ABRIL DE 2025

EB: 64322.009009/2025-92

Aprova o Manual de Campanha MC 2.40-54 Inteligência de Fontes Abertas, 1ª edição, 2025, e dá outras providências.

O **COMANDANTE DE OPERAÇÕES TERRESTRES**, no uso da atribuição que lhe confere o inciso IV do artigo 28 das Instruções Gerais para o Sistema de Doutrina Militar Terrestre – SIDOMT (EB10-IG-01.005), 7ª edição, aprovadas pela Portaria do Comandante do Exército nº 2.451, 09 de abril de 2025, resolve:

Art. 1º Aprovar o Manual de Campanha MC 2.40-54 Inteligência de Fontes Abertas, 1ª edição, 2025, que com esta baixa.

Art. 2º Determinar que esta Portaria entre em vigor na data de sua publicação.

Gen Ex ANDRÉ LUIS NOVAES MIRANDA

Comandante de Operações Terrestres

(Publicado no Boletim do Exército nº xx , de xx de xxxxxxxx de 2025)

FOLHA REGISTRO DE MODIFICAÇÕES (FRM)

NÚMERO DE ORDEM	ATO DE APROVAÇÃO	PÁGINAS AFETADAS	DATA

SUMÁRIO

PREFÁCIO

As fontes abertas sempre foram utilizadas pela Inteligência para a obtenção de dados que permitem a produção de conhecimentos e a construção de uma consciência situacional acerca de diversos temas.

O avanço da rede mundial de computadores e suas diversas inovações ampliaram o uso dessa disciplina de Inteligência, fazendo com que excedesse o ambiente físico, passando a atuar, também, no ambiente cibernético.

O grande volume de informações existente na *internet*, acessadas com riscos e custos reduzidos, fomentam, cada vez mais, o emprego dessa disciplina de Inteligência, exigindo que sua capacidade operacional seja ampliada. Nesse sentido, as Táticas, Técnicas e Procedimentos (TTP) de coleta em fontes abertas evoluem a um ritmo acelerado, para atender às Necessidades de Inteligência (NI).

Diante desse cenário, esta publicação tem como principais propósitos padronizar entendimentos, estabelecer a base conceitual e os procedimentos necessários à aplicação da Inteligência de Fontes Abertas, do inglês *Open Source Intelligence* (OSINT), como disciplina de Inteligência, observando os limites legais previstos para a atividade de Inteligência.

Para tanto, os capítulos 1 e 2 apresentam fundamentos, conceitos e terminologia específicos; já o capítulo 3 detalha a metodologia de coleta de fontes abertas e suas respectivas etapas; e, finalmente, o capítulo 4 a aborda as questões relacionadas aos riscos envolvidos na atividade, aspecto imperativo para a execução da obtenção de dados em fontes abertas.

Dessa forma, elencam-se, como público-alvo para este manual, os integrantes do estado-maior de qualquer escalão, elementos de Inteligência Militar (IM), comandantes de qualquer nível, bem como outros militares que venham a empregar a OSINT para atender às NI para apoiar o processo decisório.

CAPÍTULO I

INTRODUÇÃO

1.1 FINALIDADE

1.1.1 Apresentar conceitos e concepções da Inteligência Militar (IM) terrestre para o emprego da disciplina Inteligência de Fontes Abertas (*Open Source Intelligence – OSINT*).

1.2 CONSIDERAÇÕES INICIAIS

1.2.1 O emprego da OSINT tornou-se mais relevante com a evolução tecnológica e a popularização do acesso à *internet* e às mídias sociais. O domínio de soluções tecnológicas no Espaço Cibernético (E Ciber) tornou-se fundamental para a obtenção de dados para apoio ao processo decisório nos diversos níveis.

1.2.2 A OSINT pode ser considerada a fonte básica de Inteligência (Intlg) tendo em vista duas premissas:
a) a exploração das fontes abertas precede a utilização de quaisquer das outras disciplinas, inclusive para subsidiar o planejamento e o emprego delas; e
b) normalmente, as Necessidades de Inteligência (NI) são atendidas, total ou parcialmente, por dados de fonte aberta, tornando-as ferramentas essenciais para a obtenção da consciência situacional de quaisquer das dimensões do Ambiente Operacional (Ambi Op).

1.2.3 A coleta é a obtenção de dados disponíveis. Por disponível, entende-se o fato de o dado ser de livre acesso a quem procura obtê-lo.

1.2.4 Busca é a obtenção de dados que requer o emprego de técnica(s) operacional(is). Não é abrangida, portanto, pela Inteligência de Fontes Abertas.

1.2.5 Este manual trata, exclusivamente, das atividades relacionadas à coleta de dados.

1.3 FONTES ABERTAS

1.3.1 A OSINT, como disciplina de Intlg, baseia-se em dados coletados de fontes de obtenção de caráter público, tais como os meios de comunicação (rádio, televisão e jornais), propagandas de Estado, periódicos técnicos, manuais técnicos e livros, além daquelas livremente disponíveis no espaço cibernético.

1.3.2 A coleta de dados por fontes abertas, geralmente, envolve menos riscos, custos e meios. Nesse sentido, a OSINT deve preceder as demais fontes de obtenção para reduzir as demandas de outras disciplinas de Intlg, de maneira que estas se dediquem somente a obter dados que não possam ser adquiridos pelas fontes abertas.

"As disciplinas de Inteligência compreendem os meios, os sistemas e os procedimentos utilizados para observar, explorar, armazenar e difundir informação referente à situação, às ameaças e a outros fatores do entorno operativo. As disciplinas clássicas de Inteligência classificam-se de acordo com a ***natureza da fonte ou do órgão de obtenção*** *que a explora."*

Manual de Fundamentos Inteligência Militar Terrestre, 2ª edição, 2015 (EB20-MF-10.107).

1.4 ESPAÇO CIBERNÉTICO

1.4.1 O espaço cibernético (E Ciber) ou ciberespaço constitui um dos domínios do ambiente operacional, o qual também é composto pelos domínios marítimo, terrestre, aéreo e espacial.

1.4.2 O E Ciber é definido como o espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas por uma infraestrutura física e lógica.

1.4.3 O conceito de E Ciber abrange, ainda, as redes e os equipamentos de comunicações, além dos sistemas de informação sobre eles estabelecidos e a interação dos indivíduos com todas as camadas do ambiente.

1.4.4 O E Ciber é um ambiente complexo que extrapola os limites organizacionais e as fronteiras nacionais. Ele é resultante da interação de pessoas, *software* e serviços disponíveis na *internet*, por meio de dispositivos e redes de telecomunicações conectados a ela.

1.4.5 A *internet* é o conjunto de redes de computadores interconectados que conseguem trocar informações utilizando protocolos de comunicação, unindo usuários de todos os tipos, tais como indivíduos, instituições governamentais e privadas.

1.4.6 A *internet* representa parcela significativa tanto do E Ciber quanto das fontes abertas, como se visualiza na figura 1-1.
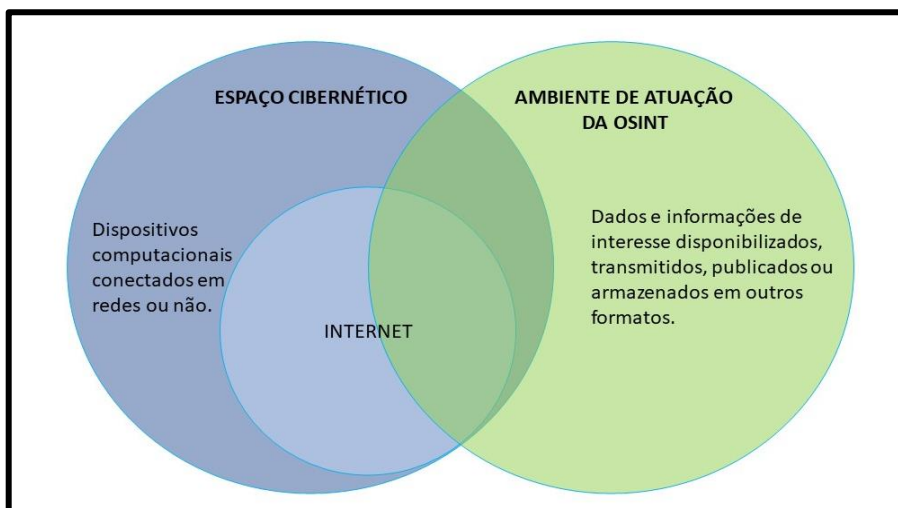
Fig 1-1 – E Ciber e o ambiente de atuação da OSINT

1.4.7 A *internet* divide-se em três camadas conceituais: *Surface Web, Deep Web* e *Dark Web*.

1.4.7.1 A *Surface Web* é composta por computadores e servidores que oferecem serviços aos seus usuários, tais como páginas *web* sem restrição de acesso, repositórios de arquivos, perfis abertos em redes sociais *etc*.

1.4.7.2 A *Deep Web* refere-se ao conteúdo que não faz parte da *Surface Web*, isto é, as informações não podem ser indexadas pelas ferramentas de coleta padrão, ou que possuem alguma restrição de acesso, como, por exemplo, páginas de instituições financeiras, de redes sociais com perfis privados e intranet de organizações.

1.4.7.3 Na *Dark Web*, além do seu conteúdo não estar indexado, possui como característica o anonimato. Entre os seus usuários, podemos destacar pessoas comuns, jornalistas, ativistas políticos, *hackers* e criminosos que se utilizam do anonimato desta camada da *internet,* beneficiando-se das possibilidades oferecidas por ela.

1.4.7.4 Ressalta-se que, dependendo do dado a ser coletado, ele pode estar em qualquer uma das três camadas da *internet*. O emprego de técnica necessária para sua obtenção definirá a especialidade requerida, para que o dado seja obtido por meio de coleta, ou busca por um elemento especializado em outra disciplina de Inteligência.

CAPÍTULO II

FUNDAMENTOS DA OSINT

2.1 INTELIGÊNCIA DE FONTES ABERTAS

2.1.1 A Inteligência de Fonte Aberta (OSINT – *Open Source Intelligence*) é aquela produzida a partir de Dados Públicos Disponíveis (DPD) e é coletada, explorada e disseminada de maneira oportuna para um público apropriado com o propósito de atender a uma Necessidade de Inteligência (NI), contribuindo para consciência situacional do Comandante (Cmt) e seu Estado-Maior (EM).

2.1.2 DPD são informações acessíveis ao público sem a necessidade do emprego de técnicas operacionais para obtê-los. Incluem conteúdo divulgado em publicações, mídia, *internet* e eventos públicos, acessíveis gratuitamente ou não, bem como dados obtidos fora do espaço cibernético, nas dimensões informacional, humana e física do Ambi Op.

2.1.3 Os dados coletados em fontes abertas podem abranger diferentes eixos temáticos, incluindo, mas não se limitando, aos seguintes exemplos:

a) mídias sociais;
b) pessoas físicas;
c) pessoas jurídicas;
d) conjuntura internacional;
e) crime organizado e terrorismo;
f) infraestruturas;
g) infraestruturas digitais; e
h) conjuntura militar internacional.

2.1.4 Os dados coletados em fontes abertas integram os documentos de Intlg, sendo essenciais para gerar consciência situacional ao comando enquadrante acerca do Ambi Op.

2.1.5 Dados e conhecimentos oriundos de fontes abertas contribuem para responder às NI, sem desconsiderar as demais disciplinas de Intlg.

2.1.6 A coleta em fontes abertas promove a ampliação do quadro de referência dos analistas de Intlg, permitindo aprofundar os conhecimentos existentes e identificar novas lacunas de dados que vão requerer outras ações para obtenção e processamento.

2.1.7 A OSINT permeia as outras disciplinas de Intlg.

2.2 POSSIBILIDADES DA OSINT

2.2.1 A OSINT, como uma das disciplinas de Intlg, envolve a coleta e a produção de conhecimentos a partir de dados de fontes abertas para a Função de Combate Inteligência, que podem ser usadas para:
a) gerar conhecimento de Intlg que auxilie no planejamento de operações militares de qualquer natureza;
b) desenvolver um quadro de referência sobre assuntos de interesse;
c) apoiar a obtenção da consciência situacional sobre ameaças e oportunidades no Ambi Op;
d) contribuir para responder às NI;
e) obter dados e produzir conhecimentos de Intlg para o Processo de Integração Terreno, Condições Meteorológicas, Inimigo e Considerações Civis (PITCIC);
f) elaborar produtos de Intlg como subsídio para o emprego das funções de combate da F Ter, apoiando os estudos em execução e o processo de tomada de decisão militar;
g) apoiar a elaboração e a atualização de dados sobre o Teatro de Operações (TO) ou Área de Operações (A Op);
h) apoiar a definição das NI que comporão o Plano de Obtenção do Conhecimento (POC), contribuindo para a identificação de lacunas de Intlg;
i) reduzir o grau de incerteza existente nos diversos ambientes operacionais;
j) contribuir com o ramo da Contrainteligência (CI); e
k) identificar a narrativa ou viés que está sendo veiculado sobre determinado fato.

2.3 LIMITAÇÕES DA OSINT

2.3.1 Para alcançar a máxima eficiência, faz-se necessário o conhecimento das NI a fim de que se estabeleçam os objetivos para o emprego da OSINT.

2.3.2 Destacam-se como principais limitações da OSINT:
a) implicação no acréscimo da capacidade de processar uma quantidade volumosa de dados;
b) implicação no acréscimo da capacidade de acompanhar a volatilidade das informações;
c) dificuldade de automatizar a coleta com base em palavras-chave e suas variações;
d) constante evolução tecnológica no Ambi Op;
e) necessidade de constante capacitação técnica dos recursos humanos para a realização da coleta;
f) necessidade de atualização dos meios de tecnologia empregados; e
g) capacidade técnica e meios empregados pelas ameaças.

2.4 COLETA EM FONTES ABERTAS

2.4.1 A coleta, sobretudo no E Ciber, requer recursos, planejamento e preparação, demandando capacidades técnicas distintas. A execução dessa atividade na Força Terrestre demanda os seguintes procedimentos prévios para sua realização:
a) acesso à *internet*;
b) recursos de segurança nos Meios de Tecnologia da Informação e Comunicações (MTIC);
c) capacitação nos eixos temáticos;
d) informações básicas sobre o assunto no qual possam subsidiar o planejamento da coleta; e
e) planejamento da gestão de riscos, conforme metodologia prevista no Capítulo V deste Manual.

2.4.2 A objetividade é muito importante na realização da coleta, uma vez que valores pessoais, sociais e culturais, fatores técnicos, dispositivos empregados, localização e o modo de acesso (navegador, termos usados, mecanismo de coleta etc.) podem influenciar os resultados.

2.4.3 A coleta deve estar em conformidade com as normas relativas ao E Ciber, sendo importante o conhecimento básico aplicável à proteção de dados e ao direito à privacidade.

2.4.4 A coleta tem como princípios metodológicos a precisão, a razoabilidade, a preservação e a segurança.

2.4.4.1 Com relação à precisão, a coleta deve se valer de fontes confiáveis e o usuário deve empregar linguagem clara, objetiva e focada em aspectos pertinentes ao tema da coleta, evitando reunir material excessivo fora do escopo a ser trabalhado.

2.4.4.2 O princípio da razoabilidade prescreve que as informações digitais só devem ser coletadas e processadas se forem:

a) justificadas por um propósito institucional;
b) estritamente necessárias para alcançar esse propósito; e
c) proporcionais à capacidade de cumprir esse propósito.

2.4.4.3 O princípio da preservação se refere à necessidade de armazenar os dados de forma tempestiva, inclusive ainda durante a coleta, de modo que evidências relevantes e potencialmente probatórias não sejam perdidas.

2.4.4.4 O princípio da segurança busca a implementação de medidas de segurança de identidade, de conexão e de ponto de acesso.

2.4.4.4.1 Alguns tipos de coleta podem ser realizados sem o uso de *internet*:
a) contato pessoal – realização de contato com pessoas relevantes ao tópico de pesquisa para a coleta de dados e opiniões de forma direta;
b) pesquisa de campo – observação e coleta de dados em locais físicos, como ambientes naturais, comunidades ou organizações;
c) observação direta – observação de comportamentos, eventos ou fenômenos e registro;
d) análise de documentos – exame de materiais impressos, como livros, revistas, jornais, relatórios e documentos de arquivo, categorizando o conteúdo para identificar padrões e tendências;
e) questionário – instrumento para coleta de dados e levantamentos censitários; e
f) grupo focal – realização de discussões em grupo para reunir opiniões, constatações e experiências dos participantes, obtendo uma compreensão mais profunda dos processos.

2.4.5 A Inteligência de Fontes Abertas é pautada pelos princípios básicos da Inteligência Militar (IM): segurança, objetividade, controle, flexibilidade, clareza, amplitude, imparcialidade, oportunidade, integração, precisão, continuidade, relevância e predição.

CAPÍTULO III

ETAPAS DA COLETA EM FONTES ABERTAS

3.1 CONSIDERAÇÕES GERAIS

3.1.1 As coletas em fontes abertas ocorrem por meio de consultas sucessivas que devem ser aperfeiçoadas durante todas as etapas da Metodologia para Produção do Conhecimento (MPC).

3.1.2 As NI são levantadas na fase de planejamento da MPC e encaminhadas à célula de OSINT durante a Fase de Gestão da Obtenção, por meio do Plano de Obtenção do Conhecimento (POC).

3.1.3 Durante as fases da MPC, as informações obtidas por meio da OSINT podem gerar novas NI, as quais devem ser novamente incluídas no POC e encaminhadas à célula de OSINT.

3.1.4 Em geral, as informações obtidas por meio da OSINT resultam em um grande volume de dados, principalmente provenientes da *internet*, o que dificulta o trabalho posterior de análise. Segue-se uma metodologia composta por etapas, cuja sequência estabelece um processo lógico que favorece a obtenção dos resultados esperados.

3.1.5 As etapas empregadas para coleta em fontes abertas são:
a) planejamento da coleta;
b) execução das coletas;
c) processamento dos dados obtidos; e
d) distribuição.

3.2 PLANEJAMENTO DA COLETA

3.2.1 A etapa de planejamento consiste na orientação da finalidade da coleta, dos recursos necessários, dos prazos disponíveis e dos riscos da atividade.

3.2.2 Após a definição pela coleta, devem ser avaliados os dados disponíveis sobre o tema/assunto, identificadas as NI que precisam ser respondidas e definidos os ambientes de atuação (humano, físico e/ou informacional), o que permitirá direcionar o esforço de obtenção. Nessa etapa, devem ser planejados os recursos necessários para as coletas, levando em consideração as necessidades técnicas para a obtenção dos dados.

3.2.3 Durante o planejamento, deve ser aplicada a metodologia para avaliação de riscos e impactos, prevista no capítulo V deste manual, com o intuito de diagnosticar o nível de risco a que o usuário será submetido e prever as medidas de segurança para a proteção dos ativos.

3.2.4 A dificuldade de acesso, o prazo estipulado e a delimitação do escopo da coleta no tempo e no espaço são fatores que devem ser levados em consideração para a definição dos meios a serem empregados.

3.2.5 O planejamento das coletas deve considerar o acesso aos dados da *internet* e outros registros.

3.2.6 As recomendações relativas aos riscos identificados na etapa anterior devem ser consideradas nas ações da etapa de planejamento.

3.2.7 Na preparação para realização de coleta em OSINT, deverão ser observados prioritariamente fóruns públicos, documentos públicos, transmissões públicas e sites da *internet.*

3.2.8 A coleta de dados em fóruns públicos exige coordenação, para garantir que a coleta esteja integrada e sincronizada com o POC e não viole leis que proíbem a coleta não autorizada de informações para fins de inteligência.

3.2.9 Para a coleta em transmissões públicas deve ser realizado o procedimento para implantar, manter, recuperar e transferir transmissões de rádio e televisão, bem como dispositivos de armazenamento de mídia e sistemas de processamento de conteúdo e comunicação. Deve ser buscado identificar recursos de coleta e processamento da *internet*, para realização de coleta em transmissões de áudio e vídeo online de estações de rádio ou televisão no ambiente virtual.

3.3 EXECUÇÃO DAS COLETAS

3.3.1 A coleta é o processo de consultas sequenciais que permite ampliar o universo de conhecimento sobre determinado assunto.

3.3.2 Durante o processo de coleta, devem ser utilizadas ferramentas que permitam a organização dos dados obtidos, de maneira a facilitar a recuperação do conteúdo coletado, atendendo ao princípio da preservação.

3.3.3 Devem ser empregadas diferentes ações, ferramentas, sistemas, *softwares* ou aplicativos para confrontar ou complementar os resultados coletados, devido às possibilidades e limitações das ferramentas de coleta.

3.3.4 A seleção das ferramentas deve levar em consideração a experiência anterior do usuário e seu quadro de referência sobre o tema, a fim de obter maior efetividade na obtenção dos dados.

3.3.5 Durante a coleta, os dados obtidos devem ser validados, analisando a credibilidade, tanto em relação à fonte quanto ao conteúdo. Para isso, deve ser realizada a Técnica de Avaliação de Dados (TAD) prevista na doutrina de IM vigente.

3.3.6 Devem ser observadas, durante a execução da coleta em Fontes Abertas, especificamente no E Ciber, as medidas cabíveis de segurança de navegação, para que as informações do usuário que está realizando a coleta sejam preservadas.

3.3.7 É de suma importância que o operador de OSINT possua o treinamento adequado para a realização de coleta em Fontes Abertas, em especial nas diversas temáticas de interesse para a produção do conhecimento de Inteligência.

3.3.8 A capacidade de reunir e analisar materiais estrangeiros é crítica na exploração de OSINT. O uso e emprego efetivos militares com habilitações em idiomas estrangeiros facilitam essa atividade. As áreas críticas das habilidades necessárias em outros idiomas são de transcrição, tradução e interpretação.

3.3.9 A utilização de Inteligência Artificial, para o desenvolvimento de sistemas de tradução e monitoramento de mídias estrangeiras deve ser observado. Este tipo de sistema proporciona ganho de tempo e efetividade, pois realiza o monitoramento de mídias estrangeiras de interesse, bem como permite que um determinado assunto seja coletado e armazenado para posterior análise ao ser transmitido em outros idiomas.

3.3.10 FONTES DE DADOS ABERTOS NA EXECUÇÃO DA COLETA

3.3.10.1 Os principais grupos de fontes de dados abertos são**:** produções acadêmicas, agências governamentais e organizações não governamentais, canais de transmissão de rádio e televisão de informação comercial ou pública, bibliotecas e centros de pesquisa e indivíduos e grupos

3.3.10.2 As principais fontes nas produções acadêmicas são: materiais didáticos, dissertações, palestras, apresentações, artigos de pesquisa e estudos em cópia impressa e eletrônica cobrindo assuntos e tópicos sobre os mais diversos temas.

3.3.10.3 As agências governamentais e organizações não governamentais podem fornecer conteúdo para coleta de: bancos de dados, informações publicadas e relatórios impressos sobre uma ampla variedade de temáticas, tais

como econômicas, ambientais, geográficas, humanitárias, de segurança e de ciência e tecnologia.

3.3.10.4 Os dados de canais de transmissão de rádio e televisão de informação comercial ou pública provém de: notícias transmitidas, publicadas e impressas em tópicos atuais internacionais, regionais e locais.

3.3.10.5 Nas bibliotecas e centros de pesquisa obtêm-se dados de: documentos impressos e bancos de dados digitais sobre uma variedade de assuntos.

3.3.10.6 Em relação aos indivíduos e grupos dados podem ser obtidos de: informações manuscritas, desenhadas, postadas, impressas e transmitidas sobre assuntos e tópicos diversos.

3.4 PROCESSAMENTO DOS DADOS OBTIDOS

3.4.1 A etapa de processamento consiste na validação e organização dos dados obtidos.

3.4.2 Os dados coletados em fontes abertas podem compor diretamente documentos previstos na doutrina de IM vigente ou serem apresentados por meio de registros para serem utilizados de forma integrada com outras fontes de Inteligência.

3.4.3 Tais registros podem conter dados e informações decorrentes de análises, monitoramentos, indicadores de alarme, manutenção e atualização de bancos de dados, informações correntes, atualizações da Ordem de Batalha, estudo de alvos, entre outros formatos, e podem ser apresentados em *briefings*, relatórios, por meio de ferramentas computacionais (interação de gráficos, imagens, bancos de dados, simulações do terreno etc.) ou documentação formal.

3.4.4 O emprego da Inteligência Artificial (IA) pode ser avaliado como ferramenta de melhoria e celeridade na análise dos dados obtidos.

3.4.5 Todo documento produzido no âmbito da Inteligência de Fontes Abertas deve seguir a MPC, inclusive a TAD.

3.4.6 APLICAÇÃO DA TAD NA INTELIGÊNCIA DE FONTES ABERTAS

3.4.6.1 Conforme o conceito de disciplina de Intlg, a Inteligência de Fontes Abertas pode coletar dados oriundos de diversas fontes. Por essa razão, a aplicação da TAD, prevista na doutrina de IM vigente, tem o objetivo de definir níveis para a idoneidade da fonte (autenticidade, confiança e competência) e para a veracidade do conteúdo (semelhança, coerência e compatibilidade).

3.4.6.2 A rápida evolução tecnológica e as técnicas de desinformação, cada vez mais elaboradas, aumentam a necessidade do uso da TAD, visando a preservar a credibilidade no assessoramento. A coleta de dados em fontes abertas deve levar em conta a possibilidade de dissimulação.

3.4.6.3 A TAD estabelece procedimentos para a aferição da credibilidade dos dados que serão utilizados como matéria-prima na produção dos conhecimentos de Intlg. Somente os dados submetidos à TAD são aproveitados para este fim, de acordo com o grau de credibilidade que lhes forem atribuídos.

3.4.6.4 A aplicação da TAD é indispensável para a produção de conhecimento de Intlg, especialmente, sobre os dados oriundos de fontes abertas. Essa aplicação deverá ocorrer durante todas as etapas da coleta.

3.4.6.5 Em virtude da grande quantidade de dados brutos a serem avaliados, podem ser utilizados *softwares* específicos para a análise da idoneidade das fontes e da veracidade dos conteúdos coletados, com o objetivo de otimizar a realização da TAD.

3.4.6.6 A Inteligência Artificial (IA) deve ser considerada na execução da TAD, pois essa vertente pode proporcionar diversas características, como por exemplo o processamento rápido e escalável, a identificação de padrões ocultos, a redução de erros humanos, a automação de processos, a análise preditiva e melhor tomada de decisão e a integração eficiente de múltiplas fontes de dados.

3.4.6.7 Deve-se acrescentar à TAD vigente, em relação à veracidade do conteúdo obtido em OSINT, os conceitos de Notícia Falsa (*Fake News*) e Desinformação. Esses conceitos podem ser identificados quando uma fonte de alto nível de idoneidade difunde dados com baixo nível de veracidade.

3.4.6.8 A Notícia Falsa refere-se à disseminação de informações falsas ou imprecisas sem a intenção de enganar. Pode ocorrer por erro, má interpretação ou falta de verificação.

3.4.6.9 A Desinformação envolve a manipulação intencional de informações para induzir outras pessoas a acreditarem em algo falso. Pode incluir *deepfakes, phishing* e táticas de desvio de atenção.

3.4.7 Os tipos de fontes usadas para avaliar informações são as fontes primárias e as fontes secundárias

3.4.8 As fontes primárias são aquelas que fornecem informações diretamente da origem, sem passar por análises ou interpretações de terceiros. Elas são consideradas mais confiáveis e autênticas porque contêm dados originais e não processados. São exemplos de Fontes primárias: sites oficiais, registros

públicos, redes sociais, documentos oficiais, imagens, vídeos, metadados e transmissões ao vivo.

3.4.9 As fontes secundárias são aquelas que interpretam, analisam ou resumem informações obtidas de fontes primárias. Elas já passaram por algum tipo de processamento, podendo incluir opiniões, interpretações ou resumos feitos por terceiros. São exemplos de Fontes secundárias: notícias, *blogs*, artigos de opinião, relatórios, pesquisas, publicações em redes sociais, livros, documentários, fóruns e podcasts.

3.4.10 O processamento dos dados obtidos das diversas mídias deve levar em conta os seguintes questionamentos: Quem está realizando a transmissão? Qual o público-alvo da transmissão? Qual o viés do canal de transmissão do dado obtido?

3.4.11 Os questionamentos acima elencados visam identificar uma possível transmissão do dado de forma direcionada, visando atingir um objetivo específico.

3.4.12 A legislação relativa aos direitos autorais e à propriedade intelectual deverá ser observada por ocasião do processamento dos dados obtidos em OSINT.

3.5 DISTRIBUIÇÃO

3.5.1 Na fase de distribuição, são divulgados os dados obtidos para o escalão que o solicitou e, ainda, mediante ordem, para quem tal conhecimento possa interessar ou ser útil.

3.5.2 A difusão dos dados pode ser feita por intermédio de vários tipos de canais de transmissão, com a finalidade de propiciar um amplo fluxo de informações, observando o princípio da oportunidade.

3.5.3 Por se tratar de dados publicamente disponíveis, os dados obtidos por meio de OSINT podem ser difundidos por formas inovadoras e seguras, inclusive verbalmente ou colaborativas, para atenderem ao princípio de oportunidade.

3.5.4 Na fase de distribuição, os dados obtidos devem ser compilados em banco de dados de OSINT, para posterior consulta em caso de necessidade.

3.5.6 Nesta fase, também devem ser observadas as questões relativas à Lei Geral de Proteção de Dados (LGPD), bem como as relativas aos direitos autorais e à propriedade intelectual.

CAPÍTULO IV

A INTELIGÊNCIA DE FONTES ABERTAS NO CONTEXTO DA INTELIGÊNCIA MILITAR

4.1 CONSIDERAÇÕES GERAIS

4.1.1 A Inteligência Militar (IM) é o conjunto de atividades e tarefas técnico-militares, exercidas em caráter permanente, que visam a produzir conhecimentos de interesse dos Cmt e seus EM, em todos os níveis, para apoiar o planejamento e o processo decisório, bem como proteger conhecimentos sensíveis, instalações, materiais e pessoal da Força Terrestre (F Ter) contra ações adversas.

4.1.2 A Inteligência de Fontes Abertas, mediante a oferta oportuna de conhecimentos e informações relevantes, proporciona condições para a análise e o julgamento de dados de interesse, ajudando a aproximar a situação percebida da situação real e a determinar as relações entre os fatores operativos e de decisão. Assim, contribui para a obtenção da consciência situacional pelos Cmt e seus EM, em todos os níveis.

4.1.3 O conhecimento de Intlg oriundo da OSINT pode ser o único ou o primeiro disponível sobre o terreno, as condições meteorológicas, as forças oponentes e as considerações civis, servindo de matéria-prima para que os integrantes dos EM possam realizar seus respectivos Exames de Situação (Exm Sit) e monitorar o andamento da situação.

4.1.4 A disponibilidade e as características dos dados coletados em fontes abertas podem variar a depender do Ambi Op. A compreensão desses aspectos é relevante para a mitigação de vieses, para o melhoramento da análise e para a correta aplicação da TAD.

4.1.5 A Inteligência de Fontes Abertas é empregada em todos os tipos de operações militares e em todas as suas fases.

4.1.6 A Inteligência de Fontes Abertas utiliza os meios, os sistemas e os procedimentos necessários para observar, explorar, armazenar e difundir informação referente à situação, às ameaças e aos outros fatores do entorno operativo.

4.1.7 A Inteligência de Fontes Abertas explora a Dimensão Informacional, especialmente, a *internet*. Contudo, não se restringe a ela, abrangendo, também, a Dimensão Física e a Dimensão Humana do Ambi Op, conforme apresentado na figura 4-1.
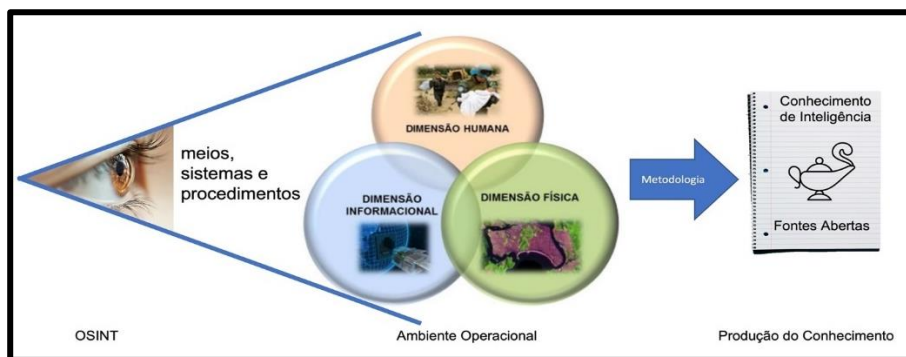
Fig 4-1 – Atuação da OSINT no Ambiente Operacional

4.1.8 A F Ter emprega seus meios de IM para atender às necessidades de conhecimento dos Cmt e seus EM nos níveis estratégico, operacional e tático. Em todos os níveis, a Inteligência de Fontes Abertas se mostra útil, quando incorporada ao Ciclo da Inteligência.

4.1.9 Os avanços tecnológicos característicos do combate moderno, associados às constantes atualizações das NI, são fatores que contribuem para otimizar a difusão do conhecimento de Inteligência, de forma a atender, com oportunidade, seus usuários nos níveis estratégico, operacional e tático.

4.1.9.1 No nível estratégico, a Inteligência de Fontes Abertas pode produzir conhecimentos, prioritariamente, sobre o oponente em suas expressões de poder. Para isso, levanta e monitora, de forma permanente, informações sobre as capacidades dos atores internacionais e as áreas de tensão internas que possam comprometer as instituições nacionais, a lei e a ordem.

4.1.9.2 No nível operacional, a Inteligência de Fontes Abertas procura obter conhecimento acerca do Ambi Op e das forças hostis presentes, ou que nele possam atuar.

4.1.9.3 No nível tático, a Inteligência de Fontes Abertas contribui para a consciência situacional, produzindo conhecimentos limitados, de curto alcance no tempo, e dirigidos às necessidades imediatas do comandante tático para o planejamento ou para a condução de operações militares. Neste nível, cresce de importância o princípio da oportunidade, visando a gerar conhecimentos e produtos descritivos, capazes de apoiar diretamente o processo decisório.

4.1.9.4 Nos níveis operacional e tático, os esforços da OSINT estão voltados para as NI de campanha militar e trabalham para apontar as vulnerabilidades do inimigo que permitam desencadear ações decisivas.

4.1.9.5 Em complemento, a Inteligência de Fontes Abertas pode auxiliar na identificação do viés ou narrativa vigente, com a finalidade de assessorar o Cmt sobre a necessidade de uma Cmp Info que atenda os Obj da Força.

4.2 EMPREGO DA INTELIGÊNCIA DE FONTES ABERTAS NO CONTEXTO DA INTELIGÊNCIA MILITAR

4.2.1 O emprego da Inteligência de Fontes Abertas contribui com a Função de Combate Inteligência (F Cmb Intlg), auxiliando na compreensão sobre: o ambiente operacional, as ameaças (atuais e potenciais), os oponentes, o terreno e as considerações civis.

4.2.2 Durante a análise das NI dos Cmt, em todos os níveis, devem ser consideradas aquelas que podem ser satisfeitas com o emprego da Inteligência de Fontes Abertas e as que demandarão o emprego de outras disciplinas de Intlg.

4.2.3 A Inteligência de Fontes Abertas pode contribuir com todas as atividades e tarefas previstas para a F Cmb Intlg, conforme a tabela 4-1.

ATIVIDADE	TAREFA
Produzir conhecimentos continuamente, em apoio ao planejamento da Força	Prover prontidão de Inteligência
	Obter dados e informações para o PITCIC
	Gerar conhecimentos de Inteligência
Executar ações de Inteligência, Reconhecimento, Vigilância e Aquisição de Alvos (IRVA)	Conduzir reconhecimentos
	Conduzir vigilância
	Conduzir outras operações e missões relacionadas à Inteligência
	Proporcionar apoio de Intlg à busca de alvos
Apoiar a obtenção da consciência situacional	Executar o PITCIC
	Acompanhar o desenvolvimento da situação
	Executar ações de Desenvolvimento da Contrainteligência em apoio à F Ter
Apoiar a obtenção da superioridade de informações	Prover apoio de Inteligência às capacidades relacionadas às informações da F Ter
	Proporcionar apoio de Inteligência às atividades de avaliação das operações
Apoio na busca de ameaças	Proporcionar apoio de Inteligência à busca continuada de ameaças
	Proporcionar apoio de Inteligência à detecção continuada de ameaças

Tab 4-1 – Atividades e tarefas da F Cmb Intlg que podem ser apoiadas pela OSINT

4.2.4 As atividades concernentes à Inteligência de Fontes Abertas são permanentes e se desenvolvem desde o tempo de paz, inseridas no Ciclo de Inteligência), apoiando o processo decisório, em uma atividade contínua e dinâmica.

4.2.5 A Inteligência de Fontes Abertas é conduzida pelo pessoal e pelos meios da F Cmb Intlg, conforme a situação. Entretanto, podem contribuir com essa disciplina todos aqueles que realizam, em determinado momento, atividades relacionadas a ela, de acordo com a figura 4-2.
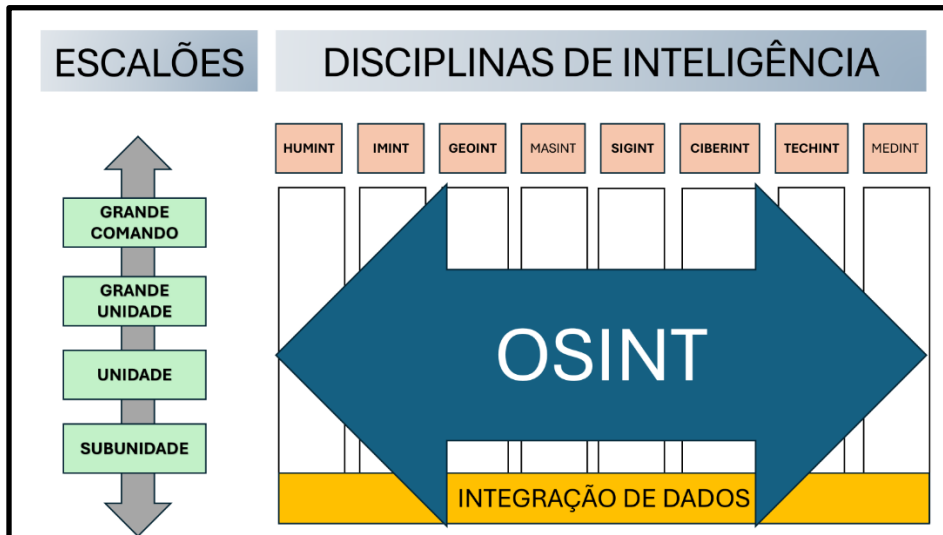
Fig 4-2 – Transversalidade da Inteligência de Fontes Abertas nas Disciplinas de Inteligência e níveis de Comando

4.3 A INTELIGÊNCIA DE FONTES ABERTAS E O CICLO DE INTELIGÊNCIA

4.3.1 A Inteligência de Fontes Abertas, no contexto da IM, é orientada pelo Ciclo de Inteligência, que compreende a Orientação, a Obtenção, a Produção e a Difusão como fases a serem cumpridas para o devido assessoramento ao processo decisório.

4.3.2 A credibilidade dos conhecimentos produzidos, especialmente, os oriundos de dados coletados em fontes abertas, depende diretamente da constante reavaliação dos procedimentos executados durante o ciclo de Inteligência, reorientando as atividades e tarefas de Intlg sempre que preciso.

4.3.3 A aderência ao ciclo de Intlg tende a garantir que todos os aspectos sobre o assunto pesquisado tenham sido considerados e a uniformizar os procedimentos para a exploração da OSINT.

4.3.4 ORIENTAÇÃO

4.3.4.1 Na Inteligência de Fontes Abertas, a fase da orientação se caracteriza pelo estabelecimento das diretrizes para o planejamento e a execução das atividades e tarefas relacionadas à coleta de dados e pela definição e priorização das NI, sendo materializada pelo planejamento do esforço de coleta no escalão considerado.

4.3.4.2 No planejamento, devem-se levar em consideração a distribuição e a estrutura dos dados em fontes abertas, de forma a mitigar conceitos pré-concebidos e auxiliar na compreensão e análise das limitações que o ambiente operacional considerado impõe.

4.3.4.3 Na execução, a Matriz de Obtenção, documento que permite o gerenciamento das ações, dos prazos e do atendimento das NI, controla se as respostas oriundas da coleta de dados em fontes abertas podem atender, total ou parcialmente, às necessidades propostas inicialmente, motivando demandas complementares ou a eventual definição de novas NI.

4.3.5 OBTENÇÃO

4.3.5.1 Na obtenção, a Inteligência de Fontes Abertas realiza a coleta baseada nas etapas previstas no capítulo III, reunindo dados, informações e conhecimentos que servirão de subsídios para a produção do conhecimento. Essa coleta ocorre por meio da exploração, sistemática ou episódica, das fontes disponíveis e da posterior entrega do material obtido aos elementos encarregados de sua transformação em conhecimentos de Intlg.

4.3.5.2 As diversas fontes existentes podem conter dados abertos ou protegidos, a Inteligência de Fontes Abertas restringe-se à reunião de dados que se encontram publicamente disponíveis, passíveis de serem obtidos por intermédio da coleta.

4.3.5.3 Os dados e as informações constantes nos registros e arquivos existentes em bancos de dados do próprio órgão ou agência de Intlg são considerados como dados já obtidos anteriormente e, portanto, devem ser reunidos na fase da Obtenção, quando forem de interesse, de forma a otimizar o esforço de coleta. Tais dados servem para compor o quadro de referência do analista, podendo-se recorrer a eles no estudo de situação de Intlg ou, até mesmo, na produção do conhecimento de Intlg. Isso não exclui a possibilidade de eventuais confirmações ou atualizações dos dados existentes, quando julgado necessário.

4.3.5.4 A fim de otimizar o tempo, após esgotada a consulta aos bancos de dados, podem ser solicitados, de modo planejado, os meios que se façam necessários para reunir dados complementares e/ou atualizados.

4.3.5.5 A fase da obtenção, na Inteligência de Fontes Abertas, é composta das seguintes etapas:

a) exploração das fontes – corresponde à realização da coleta em fontes abertas propriamente ditas, conforme descrito no capítulo anterior;

b) processamento dos dados – a fim de transformar os dados brutos, não processados, reunidos em informações inteligíveis, por meio de análises técnicas; e

c) distribuição – caracterizada pela entrega oportuna dos dados e das informações processadas aos encarregados de sua análise.

4.3.6 PRODUÇÃO

4.3.6.1 Na fase da produção, mediante a aplicação da Metodologia para a Produção do Conhecimento (MPC), os dados e informações coletados são convertidos em conhecimentos de Intlg que, no âmbito da Inteligência de Fontes Abertas, contribuem para responder às NI.

4.3.6.2 No caso da Inteligência de Fontes Abertas, enquanto disciplina elementar da atividade de Intlg, cada nova necessidade de dados pode ensejar uma reorientação do esforço de coleta, demandando novas pesquisas, em uma execução contínua do Ciclo de Inteligência. Isso pode ocorrer em função das necessidades dos Cmt e seus EM, em atendimento a um pedido ou ordem específica ou para atender ou complementar as situações anteriores.

4.3.6.3 Os dados obtidos por fontes abertas devem ser integrados com aqueles oriundos de outras fontes de obtenção, com o objetivo de aprimorar o conhecimento de Inteligência a ser produzido, atendendo ao Princípio da Integração.

4.3.6.4 A fase de produção do conhecimento pode valer-se da IA como ferramenta de propulsão das suas etapas, em especial na análise e síntese visando a integração dos dados obtidos, atendendo ao princípio da oportunidade citado anteriormente.

4.3.7 DIFUSÃO

4.3.7.1 Na fase da difusão, os conhecimentos produzidos são divulgados para o Cmt, órgão ou escalão que o solicitou e, ainda, mediante ordem, para quem o conhecimento possa interessar ou ser útil.

4.3.7.2 A difusão dos conhecimentos de Intlg é feita por intermédio de vários tipos de canais de transmissão, com a finalidade de propiciar um amplo fluxo de informações, observando o princípio da necessidade de conhecer.

CAPÍTULO V

AVALIAÇÃO E GERENCIAMENTO DOS RISCOS DA COLETA EM FONTES ABERTAS

5.1 CONSIDERAÇÕES GERAIS

5.1.1 Em que pese a Inteligência de Fontes Abertas coletar dados disponíveis ao público em geral, sua execução pode gerar riscos em virtude de excessos, desvios, incapacidade técnica, entre outros fatores. Nesse sentido, o emprego do processo de avaliação e gerenciamento dos riscos, apresenta-se como uma ferramenta capaz de diagnosticar o nível de risco que a execução da atividade está submetida e indicar medidas para o seu tratamento.

5.1.2 A avaliação e gerenciamento dos riscos da coleta em Fontes Abertas deve receber atenção especial na fase de difusão, pois apesar dos dados obtidos serem de domínio público, a análise realizada pode levar a conclusões sensíveis na dimensão informacional.

5.1.3 A adoção de medidas de segurança se trata de um processo sistemático usado para identificar, analisar e proteger informações críticas de ações que podem ser observadas por sistemas de Intlg adversários, com o objetivo de evitar que esses sistemas possam interpretar ou utilizar essas informações de forma a prejudicar as operações militares em curso ou futuras.

5.1.4 As medidas de segurança devem ser aplicadas de maneira rigorosa para proteger a execução da OSINT, garantindo que as informações críticas não sejam inadvertidamente expostas a adversários. Isso inclui a implementação de contramedidas específicas, como a criptografia de comunicações, o controle rigoroso de acesso a dados sensíveis, e a disseminação seletiva de informações apenas para aqueles que têm a necessidade de conhecer.

5.1.5 O treinamento contínuo do pessoal é essencial para garantir que todos compreendam a importância de proteger a execução da OSINT.

5.1.6 Para as coletas realizadas nas dimensões física e humana, o processo de avaliação de risco deve ser adotado de forma similar naquilo que couber, observando-se as adaptações necessárias.

5.2 PROBABILIDADE

5.2.1 A probabilidade de cada risco baseia-se em critérios para estabelecer a expectativa de um evento ocorrer. No contexto das fontes abertas, os critérios

para a determinação do nível de impacto, constantes na doutrina de Inteligência Militar vigente, são acrescidos dos critérios a seguir apresentados.

5.2.2 Para efeito do cálculo da probabilidade, deve ser considerado que a força oponente tem capacidade de monitoramento e que há motivação para a obtenção da identidade e das intenções dos especialistas de OSINT da Força Terrestre. Assim, avalia-se qual a probabilidade da força oponente acessar as ações de OSINT próprias.

PROBABILIDADE		DESCRIÇÃO E CRITÉRIOS DE OSINT
NÍVEL	**VALOR**	
MUITO BAIXA	1	**a. Descrição** - Evento com baixíssima probabilidade de comprometimento da segurança. **b. Critérios** **- Capacidade do especialista de OSINT** (conhecimento avançado nas técnicas de segurança). **- Ambiente físico** (favorável para a coleta de dados na fonte) ou no **ambiente cibernético** (coleta executada com as medidas de segurança adequadas).
BAIXA	2	**a. Descrição** - Evento com baixa probabilidade de comprometimento da segurança. **b. Critérios** **- Capacidade do especialista de OSINT** (conhecimento avançado nas técnicas de segurança). **- Ambiente físico** (desfavorável para a coleta de dados na fonte) ou **ambiente cibernético** (coleta executada com as medidas de segurança mínimas).
MÉDIA	3	**a. Descrição** - Evento com média probabilidade de comprometimento da segurança. **b. Critérios** **- Capacidade do especialista de OSINT** (conhecimento intermediário nas técnicas de segurança). **- Ambiente físico** (favorável para a coleta de dados na fonte) ou no **ambiente cibernético** (coleta executada com as medidas de segurança mínimas).

PROBABILIDADE		DESCRIÇÃO E CRITÉRIOS DE OSINT
NÍVEL	VALOR	
ALTA	4	**a. Descrição** - Evento com alta probabilidade de comprometimento da segurança. **b. Critérios** - **Capacidade do especialista de OSINT** (conhecimento intermediário nas técnicas de segurança). - **Ambiente físico** (desfavorável para a coleta de dados na fonte) ou no **ambiente cibernético** (coleta executada sem medidas de segurança).
MUITO ALTA	5	**a. Descrição** - Evento com altíssima probabilidade de comprometimento da segurança. **b. Critérios** - **Capacidade do especialista de OSINT** (sem conhecimento das técnicas de segurança). - **Ambiente físico** (para qualquer Ambi Op) ou no **ambiente cibernético** (para qualquer Ambi Op).

Tab 5-1 – Critérios para cálculo da probabilidade na avaliação do risco da coleta

5.3 IMPACTO

5.3.1 O impacto baseia-se em critérios para estabelecer a gravidade das consequências de um evento. No contexto das fontes abertas, os critérios para determinação do nível de impacto, constantes na doutrina de IM vigente, são acrescidos dos critérios a seguir apresentados:

IMPACTO		DESCRIÇÃO E CRITÉRIOS DE OSINT
NÍVEL	VALOR	
MUITO BAIXO	1	**a. Descrição** - Impactos insignificantes nos ativos da Força Terrestre. **b. Critérios** - **Imagem do Exército** (não afeta ou afeta minimamente no âmbito local). - **Operacionalidade** (não afeta a capacidade/poder de combate para o cumprimento da missão).

IMPACTO		DESCRIÇÃO E CRITÉRIOS DE OSINT
NÍVEL	VALOR	
BAIXO	2	**a. Descrição** - Impactos pequenos nos ativos da Força Terrestre. **b. Critérios** - **Imagem do Exército** (afeta negativamente, com repercussão local). - **Operacionalidade** (pequena redução da capacidade/poder de combate para o cumprimento da missão. A OM mantém a capacidade de cumprir a missão).
MÉDIO	3	**a. Descrição** - Impactos significativos nos ativos da Força Terrestre, porém recuperáveis. **b. Critérios** - **Imagem do Exército** (afeta negativamente, com repercussão regional). - **Operacionalidade** (redução da capacidade/poder de combate, podendo dificultar o cumprimento da missão).
ALTO	4	**a. Descrição** - Impactos de reversão muito difícil nos ativos da Força Terrestre. **b. Critérios** - **Imagem do Exército** (afeta negativamente, com repercussão nacional). - **Operacionalidade** (redução sensível da capacidade/poder de combate, podendo dificultar sobremaneira o cumprimento da missão).
MUITO ALTO	5	**a. Descrição** - Impactos de difícil reversão nos ativos da Força Terrestre. **b. Critérios** - **Imagem do Exército** (afeta negativamente, com repercussão internacional). - **Operacionalidade** (perda da capacidade/poder de combate para o cumprimento da missão).

Tab 5-2 – Critérios para cálculo do impacto na avaliação do risco da coleta

5.4 NÍVEL DE RISCO

5.4.1 Avaliando a relação entre a probabilidade e o impacto, o usuário é capaz de identificar o nível de risco a que será submetido ao realizar uma coleta em fontes abertas e, em consequência, adotar medidas mitigadoras.

5.4.2 O nível de risco é estabelecido mediante o emprego da matriz de exposição a riscos apresentada na figura 5-1 a seguir.

IMPACTO						
	5 MUITO ALTO	5	10	15	20	25
	4 ALTO	4	8	12	16	20
	3 MÉDIO	3	6	9	12	15
	2 BAIXO	2	4	6	8	10
	1 MUITO BAIXO	1	2	3	4	5
Níveis de risco: - EXTREMO - ALTO - MÉDIO - BAIXO		1 MUITO BAIXA	2 BAIXA	3 MÉDIA	4 ALTA	5 MUITO ALTA
		PROBABILIDADE				

EXTREMO
ALTO
MÉDIO
BAIXO

Fig 5-1 – Matriz de exposição a riscos

5.5 AVALIAÇÃO DE RISCO

5.5.1 A realização da avaliação dos riscos, além da adoção de medidas de proteção para a coleta em fontes abertas, em especial no E Ciber, contribui para o equilíbrio entre os riscos identificados e os benefícios esperados na condução da atividade. Como resultado dessa avaliação, poderão surgir restrições que devem ser levadas em consideração no planejamento e subsequente emprego dos meios de obtenção.

5.5.2 Os riscos relacionados à coleta em fontes abertas podem ser agrupados em quatro níveis: nível de risco baixo, nível de risco médio, nível de risco alto e nível de risco extremo.

5.5.2.1 Nível de risco baixo – o conhecimento das ações em fontes abertas pode representar pequenos danos para as coletas iminentes ou em curso. Deverá ser utilizado um nível mínimo de segurança. Esse nível de risco pode ser gerenciado e administrado (ACEITAR).

5.5.2.2 Nível de risco médio – o conhecimento das ações em fontes abertas representa riscos médios para as coletas iminentes ou em curso e devem ser monitorados de forma rotineira e sistemática. Esse nível de risco comporta a execução da OSINT, entretanto recomenda-se treinamento específico e exigem-se medidas adicionais de segurança (MITIGAR).

5.5.2.3 Nível de risco alto – o conhecimento das ações em fontes abertas representa riscos altos para as coletas iminentes ou em curso. Esse nível de risco comporta a execução da OSINT, desde que seja determinada por autoridade competente e com a devida justificativa (MITIGAR ou NÃO REALIZAR).

5.5.2.4 Nível de risco extremo – não comporta a execução de coleta em fontes abertas (NÃO REALIZAR).

5.5.3 O gerenciamento do risco indica as possibilidades de tratamento contidas na tabela 5-3.

TRATAMENTO	SIGNIFICADO
Aceitar	Nenhuma medida adicional é necessária, restando o monitoramento da situação.
Mitigar	Adoção de medidas mitigadoras visando a reduzir a probabilidade, o impacto dos riscos ou ambos.
Não Realizar	Abandono das atividades que geram riscos.

Tab 5-3 – Possibilidades de tratamento

5.6 MEDIDAS MITIGADORAS DE RISCOS

5.6.1 De acordo com a avaliação de riscos, devem ser implementadas medidas mitigadoras com o objetivo de preservar os ativos da Instituição. Na sequência, são apresentados exemplos de medidas mitigadoras:

a) aproveitar as bases de dados oficiais e outras disponíveis, sempre que possível, antes de iniciar a coleta de informações em fontes abertas;

b) realizar a atividade de coleta sem interação ou engajamento entre o usuário e outras pessoas, grupos ou organizações;

c) ser discreto, usar termos de coleta diversos e variar as ferramentas de coletas, alternando os padrões de tempo usados no acesso a sites e/ou locais, evitando visitar constantemente os mesmos endereços;

d) não salvar senhas no navegador e equipamento;

e) não empregar perfis ou contas particulares em *e-mails*, mídias sociais e outros serviços;
f) não realizar coletas em fontes abertas usando dispositivos de propriedade pessoal;
g) ajustar as opções de privacidade no navegador da *internet*, desativando ou monitorando a aceitação de *cookies* (dados armazenados de *sites* para acesso posterior);
h) não utilizar máquinas com resquícios de pesquisas anteriores, para evitar o seu correlacionamento; e
i) utilizar *software* antivírus e *firewall*, bem como atualização das correções de segurança dos sistemas operacionais e navegadores e outros programas da máquina.

GLOSSÁRIO

PARTE I – ABREVIATURAS E SIGLAS

A

Abreviaturas/Siglas	Significado
Ambi Op	Ambiente Operacional
A Op	Área de Operações

C

Abreviaturas/Siglas	Significado
Cmt	Comandante
CI	Contrainteligência

D

Abreviaturas/Siglas	Significado
DPD	Dados Públicos Disponíveis

E

Abreviaturas/Siglas	Significado
E Ciber	Espaço Cibernético
EM	Estado-Maior
Exm Sit	Exame de Situação

F

Abreviaturas/Siglas	Significado
F Ter	Força Terrestre
F Cmb Intlg	Função de Combate Inteligência

I

Abreviaturas/Siglas	Significado
IM	Inteligência Militar
IRVA	Inteligência, Reconhecimento, Vigilância e Aquisição de Alvos
Intlg	Inteligência

M

Abreviaturas/Siglas	Significado
MPC	Metodologia para Produção do Conhecimento de Inteligência
MTIC	Meios de Tecnologia da Informação e Comunicações
Mdt O	Mediante Ordem

N

Abreviaturas/Siglas	Significado
NI	Necessidade de Inteligência

O

Abreviaturas/Siglas	Significado
OSINT	Inteligência de Fontes Abertas (*Open Source Intelligence*)
OM	Organização Militar

P

Abreviaturas/Siglas	Significado
PITCIC	Processo de Integração Terreno, Condições Meteorológicas, Inimigo e Considerações Civis
POC	Plano de Obtenção do Conhecimento

T

Abreviaturas/Siglas	Significado
TTP	Técnicas, Táticas e Procedimentos
TAD	Técnica de Avaliação de Dados

GLOSSÁRIO

PARTE II – TERMOS E DEFINIÇÕES

Ontologia Textual – Modelo representado por uma estrutura de dados. Esta estrutura é composta por termos, relações entre termos e axiomas que descrevem a relação entre eles. As ontologias textuais podem ser usadas para melhorar a precisão e a relevância das coletas em fontes abertas.

Operador Lógico – Termo ou símbolo que permite a combinação de expressões ou palavras-chave nos mecanismos de busca.

Palavra-chave – Termo ou expressão que resume os temas principais de um tema e servem de referência para pesquisas.

REFERÊNCIAS

BRASIL. Exército. Comando de Operações Terrestres. **Planejamento e Emprego da Inteligência Militar.** EB70-MC-10.307. 1. ed. Brasília, DF: COTER, 2016.

BRASIL. Exército. Comando de Operações Terrestres. **Guerra Cibernética**. EB70-MC-10.232. 1. ed. Brasília, DF: COTER, 2017.

BRASIL. Exército. Comando de Operações Terrestres. **Contrainteligência.** EB70-MC-10.220. 1. ed. Brasília, DF: COTER, 2019.

BRASIL. Exército. Comando de Operações Terrestres**. Operações de Informação.** EB70-MC-10.213. 2. ed. Brasília, DF: COTER, 2019.

BRASIL. Exército. Comando de Operações Terrestres. **Produção do Conhecimento de Inteligência.** EB70-MT-10.401. 1. ed. Brasília, DF: COTER, 2019.

BRASIL. Exército. Comando de Operações Terrestres. **Inteligência Cibernética**. EB70-MC-10.356. Edição Experimental. Brasília, DF: COTER, 2020.

BRASIL. Exército. Comando de Operações Terrestres. **Caderno de Instrução Táticas, Técnicas e Procedimentos da Tropa como Sensor de Inteligência.** EB70-CI-11.465. 1. ed. Brasília, DF: COTER, 2021.

BRASIL. Exército. Comando do Exército. **Instruções Gerais para as Publicações Padronizadas do Exército**. EB10-IG-01.002. 1. ed. Brasília, DF: C Ex, 2011.

BRASIL. Exército. Comando do Exército. **Instruções Gerais para a Salvaguarda de Assuntos Sigilosos**. EB10-IG-01.011. 2. ed. Brasília, DF, 2023.

BRASIL. Exército. Estado-Maior do Exército. **Inteligência.** EB20-MC-10.207. 1. ed. Brasília, DF: EME, 2015.

BRASIL. Exército. Estado-Maior do Exército. **Inteligência Militar Terrestre.** EB20-MF-10.107. 2. ed. Brasília, DF: EME, 2015.

BRASIL. Exército. Estado-Maior do Exército. **Doutrina Militar Terrestre**. EB20-MF-10.102. 3. ed. Brasília, DF: EME, 2019.

BRASIL. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. **Glossário das Forças Armadas.** MD35-G-01. 5. ed. Brasília, DF: MD, 2015.

BRASIL. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. **Manual de Abreviaturas, Siglas, Símbolos e Convenções Cartográficas das Forças Armadas.** MD33-M-02. 4. ed. Brasília, DF: MD, 2021.

LEAL, Luís H. **CYBINT x OSINT: Semelhanças, Diferenças e Responsabilidades**. Revista EsIMEx: A Lucerna, ano VIII. Brasília, DF, 2019.

OLIVEIRA, Jorge A. H. **A Produção do Conhecimento de Inteligência no Exército Brasileiro em Face das Necessidades de Inteligência Corrente e Prospectiva**. EsIMEx. Brasília, 2023.

USA. United States Army. ***Open Source Intelligence, ATP 2-22.9*****.** United States Army Publishing Directorate, 2019.